

Práctica 7.2 Creación de una VPC en AWS Learner Lab

miércoles, 26 de febrero de 2025 16:41

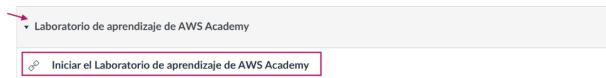
Escenario

Se requiere la creación de una **VPC personalizada** con el siguiente esquema de red:

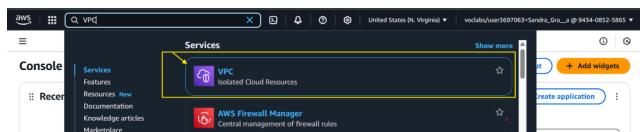
- **Rango de red de la VPC:** 10.20.0.0/16
- **Número total de subredes:** 6
 - **2 subredes públicas** (una en cada zona de disponibilidad)
 - **4 subredes privadas** (dos a dos en una misma zona de disponibilidad)
- Configurar y probar el acceso a Internet para las subredes públicas mediante un **Internet Gateway**.
- Configurar y probar la conectividad a Internet para al menos dos subredes privadas a través de un **NAT Gateway**.

Pasos/enunciados

1. Dibuja un **esquema** de la VPC del problema descrito.
2. Inicia sesión en el aula virtual de AWS **Academy Learner Lab** y accede al apartado Lanzamiento del Laboratorio para el alumnado de AWS Academy.



3. Accede al servicio de **VPC**.



4. Crea una **nueva VPC** con los siguientes valores:

- **Nombre:** VPC-NombreEstudiante
- **Rango de CIDR:** 10.20.0.0/16
- **Sin bloque IPv6**
- **Tenencia:** Predeterminado

The screenshot shows the 'Create VPC' wizard in the AWS Cloud Console. The first step, 'VPC settings', is completed. It shows the 'Name tag - optional' field with 'VPC-SandraGraña' and the 'IPv4 CIDR block' field with '10.20.0.0/16'. The second step, 'IPv6 CIDR block', is partially visible. The third step, 'Tags', is also partially visible at the bottom.

VPC settings

Resources to create: VPC only VPC and more

Name tag - optional: VPC-SandraGraña

IPv4 CIDR block: 10.20.0.0/16

IPv6 CIDR block

No IPv6 CIDR block IPAM-allocated IPv6 CIDR block Amazon-provided IPv6 CIDR block IPv6 CIDR owned by me

Tenancy: Default

Tags: A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name Value - optional: VPC-SandraGraña

Add tag

Create VPC

5. Crea las 6 **subredes** indicadas en este apartado y la **tabla** siguiente:
- Crear **2 subredes públicas** llamadas *subred-publica-1* y *subred-publica-2* distribuyéndolas en diferentes zonas de disponibilidad (por ejemplo, *us-east-1a* y *us-east-1b*).
 - Crear **4 subredes privadas**, llamadas *subred-privada-[1-4]* distribuyéndolas dos a dos en dos zonas de disponibilidad diferentes.
 - Deberás de dividir la red en segmentos más pequeños que utilicen su propia máscara de subred para un total de **251** posibles instancias cada una y especificarlo en el **Rango CIDR**.

Nombre	Tipo	Zona disponibilidad	Rango CIDR
subred-publica-1	Pública	us-east-1a	10.20.1.0/24
subred-publica-2	Pública	us-east-1b	10.20.2.0/24
subred-privada-1	Privada	us-east-1a	10.20.3.0/24
subred-privada-2	Privada	us-east-1a	10.20.4.0/24
subred-privada-3	Privada	us-east-1b	10.20.5.0/24
subred-privada-4	Privada	us-east-1b	10.20.6.0/24

Utilizamos una máscara de subred **/24** (que permite hasta 254 hosts, restando direcciones reservadas para la red y el gateway).

Pasos para crear:

1. Create Subnet
2. Elegir VPC
3. Crear cada subred con:
 - i. Su nombre
 - ii. Su zona
 - iii. Su CIDR Rango
4. Add new Subnet

The screenshot shows the AWS VPC Subnets creation interface. It displays three separate 'Create subnet' forms, each with the following fields filled in:

- VPC ID:** vpc-02ba0351f2c898f78 (VPC-SandraGraña)
- Associated VPC CIDRs:** IPv4 CIDRs: 10.20.0.0/16
- Subnet settings:**
 - Subnet name:** subred-publica-1
 - Availability Zone:** United States (N. Virginia) / us-east-1a
 - IPv4 VPC CIDR block:** 10.20.0.0/16
 - IPv4 subnet CIDR block:** 10.20.1.0/24
 - Tags - optional:** Name: subred-publica-1
- Subnet 2 of 2:**
 - Subnet name:** subred-privada-2
 - Availability Zone:** United States (N. Virginia) / us-east-1b
 - IPv4 VPC CIDR block:** 10.20.0.0/16
 - IPv4 subnet CIDR block:** 10.20.2.0/24
 - Tags - optional:** Name: subred-privada-2

The top navigation bar shows 'Subnets (6)' and the bottom navigation bar shows 'VPC > Subnets > Create subnet'.

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="subred-privada-1"/> <input type="button" value="Remove"/>

You can add 49 more tags.

VPC > Subnets > Create subnet

Subnet 4 of 4

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="subred-privada-2"/> <input type="button" value="Remove"/>

You can add 49 more tags.

VPC > Subnets > Create subnet

Subnet 5 of 6

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="subred-privada-3"/> <input type="button" value="Remove"/>

You can add 49 more tags.

VPC > Subnets > Create subnet

Subnet 6 of 6

Subnet name
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
 256 IPs

Tags - optional

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="subred-privada-4"/> <input type="button" value="Remove"/>

You can add 49 more tags.

VPC > Subnets > Create subnet

aws Search [Alt+S] United States (N. Virginia) vocabs/

VPC dashboard < You have successfully created 6 subnets: subnet-098dac2c6fbdb59a1, subnet-0352cc6846f6e4359, subnet-0fe8e5fcefe8f11ac, subnet-01e3a750c076b6f43, subnet-02b6cfe008c2c7559, subnet-070c10cb559e3cba1 >

6. Crear y configurar un **Internet Gateway (IGW)**
 - a. Crea un **Internet Gateway** en el puertos de enlace de Internet llamado IGW-MiVPC-NombreEstudiante
 - b. Una vez que lo has creado adjúntalo a tu VPC desde el listado de Gateways.

aws Search [Alt+S] United States (N. Virginia) vocabs/user3697063=Sandra_Gra_a @ 9434-0852-5865

Subnets Route tables Internet gateways Actions

Internet gateways (1) Info

Create internet gateway Info
An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

7. Crea y asociar **tablas de enruteamiento** para las **subredes públicas**.
- Crear dos nuevas tablas de rutas para cada subred pública, llamadas RT1-Pública y RT2-Pública.
 - En el apartado **asociaciones de subred** asignarlas a sus correspondientes subredes públicas.
 - En cada tabla creada, ve a **agregar ruta** y añade lo siguiente:
 - Destino:** 0.0.0.0/0
 - Target:** Puerta de enlace de Internet (el IGW creado en el paso anterior).

Pasos:

- Create Route Table:
 - Nombre
 - VPC
- Seleccionar Tablas e ir a Route Associations

Route tables (1/4) Info

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0afdechd007e53b5a	-	-	Yes	vpc-0b37a8f;
-	rtb-0989321e34033574e	-	-	Yes	vpc-02ba033
RT1-Pública	rtb-05d17b2b45a8c0b9b	-	-	No	vpc-02ba033
-	rtb-04091ce2209661965	-	-	No	vpc-02ba033

rtb-05d17b2b45a8c0b9b / RT1-Pública

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (0)

Edit subnet associations

RT2-Pública : Subnet Associations

RT2-Pública : Subnet Associations

Route tables (1/4) Info

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
-	rtb-0afdechd007e53b5a	-	-	Yes	vpc-0b37a8f;
-	rtb-0989321e34033574e	-	-	Yes	vpc-02ba033
RT1-Pública	rtb-05d17b2b45a8c0b9b	subnet-098dac2c6fbdd59a1	-	No	vpc-02ba033
RT2-Pública	rtb-04091ce2209661965	-	-	No	vpc-02ba033

rtb-04091ce2209661965 / RT2-Pública

Details | Routes | **Subnet associations** | Edge associations | Route propagation | Tags

Explicit subnet associations (0)

Edit subnet associations

8. Crear y configurar un **NAT Gateway**.
- Crea un **NAT Gateway** llamado NAT-MiVPC-NombreEstudiante
 - En el apartado subred indica una subred pública dentro de tu VPC (**Nota importante:** los **NAT Gateways van configurados a una red pública para dar salida de la subred a Internet**)
 - En el apartado **dirección IP elástica**, crear una **nueva**.
Al hacer clic en crear, en NAT tardará un momento en crearse (aparecerá en estado **pending**)

Pasos:

- Create NAT Gateway:
 - Nombre
 - Asociar Subred Pública
 - Indicar tipo
 - dirección IP elástica (Allocate)

NAT gateways info

Create NAT gateway

VPC dashboard

NAT gateways

Actions

VPC > NAT gateways > Create NAT gateway

Create NAT gateway Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

NAT gateway settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.
NAT-MIVPC-SandraGraña

The name can be up to 256 characters long.

Subnet
Select a subnet in which to create the NAT gateway.
subnet-098da2c6fb0d59a1 (subnet-publica-1)

Connectivity type
Select a connectivity type for the NAT gateway.
Public

Elastic IP allocation ID - Info
Assign an Elastic IP address to the NAT gateway.
epaloc-0f01087f57b0b2ca

Additional settings Info

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional
Q Name Q NAT-MIVPC-SandraGraña Remove Add new tag

You can add 49 more tags.

Cancel Create NAT gateway

9. Asociar al menos dos subredes privadas al NAT Gateway

- **Modificar las tablas de rutas de las subredes privadas:**
 - Dirígete al apartado **tablas de enrutamiento** del panel lateral izquierdo.
 - Crea una nueva tabla de rutas para las subredes privadas llamada RT-Privada
 - En **asociaciones de subredes**, asigna las siguientes subredes privadas a la tabla:
 - subred-privada-1
 - subred-privada-2
- **Configurar la ruta para el tráfico de Internet:**
 - En la tabla de rutas creada, accede a la pestaña **rutas** y haz clic en editar rutas.
 - Añade la tabla creada, agrega la siguiente **regla**:

Destino: 0.0.0.0/
Target: Puerta de enlace NAT (el NAT Gateway creado en el paso anterior).

Creación de tabla enrutamiento privada: RT-Privada

aws Search [Alt+5] United States (N. Virginia) vocation/user5697063=Sandra_Gra_a @ 9434-0852-3865

VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Route table settings

Name - optional
Create a tag with a key of 'Name' and a value that you specify.
RT-Privada

VPC
The VPC to use for this route table.
vpc-02ba0331f2c898f78 (VPC-SandraGraña)

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional
Q Name Q RT-Privada Remove Add new tag

You can add 49 more tags.

Cancel Create route table

Asociación de Subredes:

✓ You have successfully updated subnet associations for rtb-041b45d331a042f8a / RT-Privada.

rtb-041b45d331a042f8a / RT-Privada Actions ▾

Details Info

Route table ID rtb-041b45d331a042f8a	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-02ba0331f2c898f78 VPC-SandraGraña	Owner ID 943408525865		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
subred-privada-1	subnet-0fe8e5fceef6f11ac	10.20.3.0/24	-
subred-privada-2	subnet-01e3a750c076b6f43	10.20.4.0/24	-

Edit subnet associations

aws Search [Alt+5] United States (N. Virginia) vocation/user5697063=Sandra_Gra_a @ 9434-0852-3865

VPC > Route tables > rtb-041b45d331a042f8a > Edit subnet associations

Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
subred-privada-3	subnet-02b6fcfe008c2c7559	10.20.5.0/24	-	Main (rtb-0989321e34033574e)
subred-privada-1	subnet-0fe8e5fceef6f11ac	10.20.3.0/24	-	Main (rtb-0989321e34033574e)
subred-publica-2	subnet-0352cc5846f6e4359	10.20.2.0/24	-	rtb-04091ce2209661965 / RT2-Public
subred-publica-1	subnet-098da2c6fb0d59a1	10.20.1.0/24	-	rtb-05617fb2a5af0fb / RT1-Public
subred-privada-4	subnet-070e10b359e5cba1	10.20.6.0/24	-	Main (rtb-0989321e34033574e)
subred-privada-2	subnet-01e3a750c076b6f43	10.20.4.0/24	-	Main (rtb-0989321e34033574e)

Selected subnets
subnet-0fe8e5fceef6f11ac / subred-privada-1 subnet-01e3a750c076b6f43 / subred-privada-2

Cancel Save associations

Ruta para el tráfico:

The screenshot shows the AWS VPC Route Tables interface. At the top, there's a success message: "You have successfully updated subnet associations for rtb-041b45d331a042f8a / RT-Privada." Below this, the route table details are shown: Route table ID (rtb-041b45d331a042f8a), Main (No), Owner ID (943408525865), and VPC (vpc-02ba0331fc898f78 | VPC-SandraGrafa). The 'Routes' tab is selected, showing one route (Destination: 10.20.0.0/16, Target: local, Status: Active, Propagated: No). Below this, the 'Edit routes' section allows adding new routes. A red box highlights the 'Edit routes' button. An arrow points from the 'Edit routes' button to the 'Edit routes' section. Another arrow points from the 'Edit routes' section to the 'Save changes' button.

10. Revisa y prueba la **conectividad** con dos instancias de prueba.

- Lanza una instancia en una **subred pública** para verificar la conectividad a Internet.
 - Crea una instancia en **EC2** de Amazon Linux por ejemplo y llámala **Instancia-publica-NombreEstudiante**
 - No te olvides seleccionar un par de claves de inicio de sesión.
 - En el apartado de **configuraciones de red**:
 - Selecciona la VPC que creaste anteriormente.
 - Selecciona una subred pública de las que creaste.
 - Habilita asignar automáticamente la IP pública.
 - En **configuración de red avanzada** escribe en IP principal una de la del rango de la subred pública que hayas seleccionado.
 - Conéctate a la instancia y desde la consola y haz ping a www.google.com y si funciona es que todo está bien configurado.
- Lanza una instancia en una **subred privada** para verificar que pueda salir a Internet a través del NAT Gateway.
 - Crea una nueva instancia siguiendo los pasos anteriores y llámala **Instancia-privada-NombreEstudiante**
 - En el apartado de **configuraciones de red**:
 - Selecciona ahora una **subred privada** con acceso al NAT Gateway de las que creaste.
 - Desactiva la opción de asignar automáticamente una IP pública, ya que la instancia estará en una subred privada.
 - En **configuración de red avanzada** escribe en IP principal una de la del rango de la subred privada que hayas seleccionado.
 - Conéctate a la instancia y verifica hacer ping a una dirección para comprobar si se puede acceder a la red.

Para ambas instancias tienes que entrar en EC2:

The screenshot shows the AWS EC2 Instances dashboard. On the left, the navigation menu includes Services (selected), Features, Resources (New), Documentation, and Knowledge articles. The main area shows the EC2 service icon with the subtext "Virtual Servers in the Cloud". Below this, the "Instances" section has a "Find Instance by attribute or tag (case-sensitive)" search bar and filters for Instance state, Instance type, Status check, and Availability Zone. A message states "You do not have any instances in this region". At the bottom, there's a "Select an instance" button. A red box highlights the "EC2" service icon. An arrow points from the "EC2" service icon to the "Launch instances" button. Another arrow points from the "Launch instances" button to the "Launch instances" button in the "Instances info" section.

INSTANCIA PARA SUBRED PUBLICA:

The screenshot shows the AWS EC2 Launch instance wizard. The first step is "Launch an instance". It includes a summary of the instance configuration: Number of instances (1), Software Image (AMI) (Amazon Linux 2023.6.2...), and a note about the instance type (t2.micro). The "Name and tags" section is expanded, showing a "Name" input field containing "Instancia-publica-SandraGrafa". A red box highlights the "Name and tags" section. An arrow points from the "Name and tags" section to the "Name" input field. Another arrow points from the "Name" input field to the "Software Image (AMI)" section.

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Quick Start

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes):

Launch instance [Preview code](#)

Summary

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2... [read more](#)

Virtual server type (instance type): t2.micro

Firewall (security group): New security group

Storage (volumes): 1 volume(s) - 8 GiB

Launch instance [Preview code](#)

Instance type [Info](#) | Get advice

Instance type: t2.micro

Family: t2 - 1 vCPU 1 GiB Memory Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required: vockey

Create new key pair

* También está la opción de crear un nuevo par de claves (Recomendable)

Network settings [Info](#)

VPC - required: [Info](#) **vpc-02ba0331f2c898f78 (VPC-SandraGrána)**

Subnet: [Info](#) **subnet-098dac2c6fbdb59a1**

Auto-assign public IP: [Info](#) **Enable**

Firewall (security groups): [Info](#) **Create security group**

Advanced network configuration

Network interface 1

Device index: 0

Network interface: [Info](#) **New interface**

Description: [Info](#)

Subnet: [Info](#) **subnet-098dac2c6fbdb59a1**

Primary IP: [Info](#) **10.20.1.6**

Secondary IP: [Info](#) **Select**

IPv6 IPs: [Info](#) **Select**

IPv4 Prefixes: [Info](#) **Select**

IPv6 Prefixes: [Info](#) **Select**

Assign Primary IPv6 IP: [Info](#) **Select**

Delete on termination: [Info](#) **Select**

* Al poner la IP ten en cuenta de que las 5 primeras están reservadas. Así que usa .6 o .7

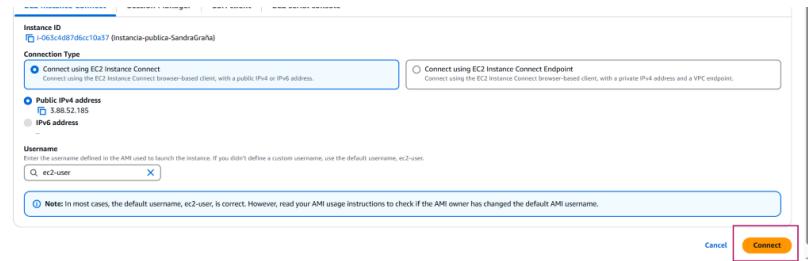
CONEXION INSTANCIA PUBLICA:

EC2 > Instances > i-063e4d87d6c10a37 > Connect to instance

Connect to instance [Info](#)

Connect to your instance i-063e4d87d6c10a37 (Instancia pública-SandraGrána) using any of these options

EBS Instance Storage | Session Manager | SSH Client | EC2 Serial Console



```

-- V=1.1>
~~~ /m/
[ec2-user@ip-10-20-1-7 ~] ping www.google.com
PING www.google.com (172.253.115.104) 56(84) bytes of data.
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=1 ttl=58 time=2.46 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=2 ttl=58 time=2.24 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=3 ttl=58 time=2.76 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=4 ttl=58 time=2.40 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=5 ttl=58 time=2.34 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=6 ttl=58 time=2.34 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=7 ttl=58 time=2.00 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=8 ttl=58 time=2.04 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=9 ttl=58 time=2.22 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=10 ttl=58 time=2.04 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=11 ttl=58 time=1.92 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=12 ttl=58 time=2.58 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=13 ttl=58 time=1.92 ms
64 bytes from bg-in-104.1e100.net (172.253.115.104): icmp_seq=14 ttl=58 time=1.91 ms

```

INSTANCIA PARA SUBRED PRIVADA:

Nombre: Instancia-privada-Sandra

AMI: Amazon Linux (Porque esta EC2 Instance Connect habilitado por defecto)

Usaremos el username para conectarnos: e2-user

Tipo de Instancia: Defecto

Crear par de claves

Configuración de red:

- VPC: Selecciona la VPC donde configurarás el NAT Gateway
- Subred: Selecciona una subred privada con acceso al NAT Gateway

- Asignar IP pública automáticamente: Desactivado

Grupo de seguridad:

- Permitir conexión SSH (puerto 22) desde la subred pública o desde un VPC Endpoint
- Permitir tráfico de salida a Internet (0.0.0.0/0)

The screenshot shows the AWS EC2 Instances launch wizard. In the 'Network settings' section, a red box highlights the 'Subnet' dropdown set to 'subnet-01e3a750c076b6f43'. Another red box highlights the 'Inbound Security Group Rules' section, specifically the first rule: 'Security group rule 1 (TCP, 22, 10.20.0.0/16)'. A red arrow points from the subnet dropdown to the source IP field in this rule. Below it, another red box highlights the second rule: 'Security group rule 2 (All, All, 0.0.0.0/0)', with a red arrow pointing from its type dropdown to the source IP field.

* IP privada: Escribe una IP dentro del rango de la subred privada (10.0.4.7)

Advanced network configuration

The screenshot shows the 'Advanced network configuration' section. It includes fields for 'Device index' (0), 'Network interface' (New interface), 'Description' (Info), 'Subnet' (subnet-01e3a750c076b6f43), 'Security groups' (New security group), 'Primary IP' (Info, value: 10.20.4.7), 'Secondary IP' (Select), 'IPv6 IPs' (Select), 'IPv4 Prefixes' (Select), 'IPv6 Prefixes' (Select), 'Assign Primary IPv6 IP' (Info, Select), and 'Delete on termination' (Select). A red box highlights the 'Primary IP' field, and a red arrow points from the 'Subnet' dropdown to the 'Primary IP' field.

CONEXION INSTANCIA PRIVADA:

The screenshot shows the final step of the EC2 Instances launch wizard. A green success message at the top says 'Success Successfully initiated launch of instance (i-0cbfb95d2a1f4ed471)'. Below it, a 'Next Steps' section lists several options: 'Create billing and free tier usage alerts' (with a 'Create billing alerts' button), 'Connect to your instance' (with 'Connect to instance' and 'Learn more' buttons), 'Connect an RDS database' (with 'Connect an RDS database' and 'Create a new RDS database' buttons), and 'Create EBS snapshot policy' (with a 'Create EBS snapshot policy' button). A red box highlights the success message, and a red arrow points from the 'Primary IP' field in the previous screenshot to the success message here.

Ahora hay que crear un ENDPOINT en VPC:

- Nombre (Instancia-Privada-Sandra)
- Elegir el tipo con interfaz para EC2 instance connect (Que es de donde nos conectaremos)
- Elegir la VPC donde está la subred privada
- Elegir el grupo de seguridad que has usado en la instancia (En mi caso es la 5)
- Elegir la subred privada que está en la instancia

The screenshot shows the AWS VPC Endpoints service. A red box highlights the 'Endpoints' section, and a red arrow points from the 'Create EBS snapshot policy' button in the previous screenshot to the 'Endpoints' section here.

Screenshot of the AWS VPC Endpoint service configuration page. It shows a search bar and a table with columns: Name, VPC endpoint ID, Endpoint type, Status, and Service. A message indicates "No endpoint found". Below the table, a section titled "Select an endpoint" is shown.

Endpoint settings:
 Specify a name and select the type of endpoint.
Name tag - optional:
 Create a tag with a key of "ServiceName" if a value that you specify. Tags help you find and manage your endpoint.
Endpoint-Private-Sandra

Type: EC2 Instance Connect Endpoint
 An elastic network interface that allows you to connect to resources in your VPC.

Network settings:
 Select the VPC in which to create the endpoint.
 vpc-02ba0351f2c898f78 (VPC-SandraGrafa)

Additional settings:

Security groups (1/6) info:
 VPC: vpc-02ba0351f2c898f78
 Group ID: sg-0c5056e9965c61a00
 Subnet: subnet-01e3a750c7b6b6f43 (subnet-privada-2)
 Tags: Name: Endpoint-Private-Sandra

Create endpoint

Endpoints (1/1) info:
 Introducing two new types of endpoints: Resource endpoint and Service network endpoint.
 Use a Resource endpoint to access a VPC resource (ARN-based resource, domain name and IP address) in another VPC. Use a Service network endpoint to access a VPC's private service network. Learn more
 Endpoints (1/1) Actions Create endpoint
 Name: Endpoint-Private-Sandra | VPC endpoint ID: eice-0b42993285803903f | Endpoint type: EC2 Instance Connect Endpoint | Status: Available

Connect to instance:
 Connect to your instance (i-0b95d2a3f4a4d471) (Endpoint-Private-Sandra) using one of these options:
 EC2 Instance Connect Session Manager SSH client EC2 serial console
 Connection type: Connect using EC2 Instance Connect
 Private IP Address: i-0b95d2a3f4a4d471 (Endpoint-Private-Sandra)
 EC2 Instance Connect Endpoint (Only endpoints that have compatible creation options can be selected. The process can take up to 15 minutes. If you create an endpoint, refresh this list to check it in the available status.)
 Username: ec2-user
 Max tunnel duration (seconds): 3600
 Max tunnel duration (seconds): 3600

CONEXION A INSTANCIA PRIVADA CON SSH Y BASTION:

Crear instancia Bastion, necesitas:

- VPC de la instancia privada
- Mismo par de claves
- Dirección IP publica auto
- SSH

Después en la instancia privada:

- Debes de poner en el grupo de seguridad SSH con origen: IP del bastion host.

IP Pública del Bastion en la instancia privada:

CONEXION CON SSH EN TERMINAL CMD:

- Debes estar en la carpeta donde está el par de llaves, en mi caso es en Downloads
- Copia el par de llaves en la instancia bastion:
 - scp -i "privadallaves.pem" privadallaves.pem ec2-user@23.20.220.140:~
- Entra en la instancia bastion con ssh:

- ssh -i "privadallaves.pem" [ec2-user@23.20.220.140](#)
- Aquí dale permisos (te lo pide aws): chmod 400 para esconderlo
- Conectate con SSH a la instancia privada:
 - Puedes hacer ping a su ip privada para asegurarte de que lo vea.
 - ssh -i "privadallaves.pem" [ec2-user@10.20.4.7](#)

```

ec2-user@ip-10-20-4-7:~ % + v

C:\Users\Sandra\Downloads>scp -i "privadallaves.pem" privadallaves.pem ec2-user@23.20.220.140:~/privadallaves.pem
100% 1678 15.2KB/s 00:00

C:\Users\Sandra\Downloads>ssh -i "privadallaves.pem" ec2-user@23.20.220.140
# 
#_###_ Amazon Linux 2023
#\_\_\_#####
#\_ \###| https://aws.amazon.com/linux/amazon-linux-2023
#\_ \#/ -->
#\_ V~' :>
#\_ /-
#\_ /_/
#\_ /_/
Last login: Wed Mar 19 19:20:48 2025 from 80.38.38.148
[ec2-user@ip-10-20-1-24 ~]$ chmod 400 privadallaves.pem
[ec2-user@ip-10-20-1-24 ~]$ ssh -i "privadallaves.pem" ec2-user@10.20.4.7
# 
#_###_ Amazon Linux 2023
#\_\_\_#####
#\_ \###| https://aws.amazon.com/linux/amazon-linux-2023
#\_ \#/ -->
#\_ V~' :>
#\_ /-
#\_ /_/
#\_ /_/
[ec2-user@ip-10-20-4-7 ~]$ 

/_/ -/
/_/m/` 

[ec2-user@ip-10-20-4-7 ~]$ ping www.google.com
PING www.google.com (172.253.122.105) 56(84) bytes of data.
64 bytes from bh-in-f105.1e100.net (172.253.122.105): icmp_seq=1 ttl=104 time=3.08 ms
64 bytes from bh-in-f105.1e100.net (172.253.122.105): icmp_seq=2 ttl=104 time=2.53 ms
64 bytes from bh-in-f105.1e100.net (172.253.122.105): icmp_seq=3 ttl=104 time=2.50 ms
64 bytes from bh-in-f105.1e100.net (172.253.122.105): icmp_seq=4 ttl=104 time=2.31 ms
64 bytes from bh-in-f105.1e100.net (172.253.122.105): icmp_seq=5 ttl=104 time=2.32 ms
64 bytes from bh-in-f105.1e100.net (172.253.122.105): icmp_seq=6 ttl=104 time=2.53 ms
^C
--- www.google.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
rtt min/avg/max/mdev = 2.313/2.545/3.080/0.256 ms
[ec2-user@ip-10-20-4-7 ~]$ 

```